
Safing

アジェンダ

- 自己紹介
- 弊社概要
- Safingサービス概要
- AWSセキュリティの考え方
- Safingの仕組み
- Safingで出来ること
- ご活用イメージ/ユースケース
- 料金プラン
- 申込方法/トライアルのご案内

スピーカー紹介

大田原 慶道 （Yoshimichi Ohtahara）

所　属

JIG-SAW株式会社
アカウントマネジメント本部　本部長

セールス、アーキテクト、マーケティングのマネジメント、
お客様のクラウド活用における技術的な課題の解決を支援する業務に従事

池川 健太郎 （Kentaro Ikegawa）

所　属

JIG-SAW株式会社
アカウントマネジメント本部　マネージャー

自社開発のセキュリティサービス「Safing」の事業推進

JIG-SAW

会社紹介

社名
JIG-SAW株式会社

設立
2001年11月1日

ISMS認証
IR0038
(ISO/IEC27001:2013,JIS Q 27001:2014)

上場市場
東京証券取引所グロース
(証券コード3914)

本社
東京都千代田区大手町1丁目9番2号
大手町フィナンシャルシティグランキューブ18F

拠点
東京・札幌・盛岡・トロント・サンフランシスコ

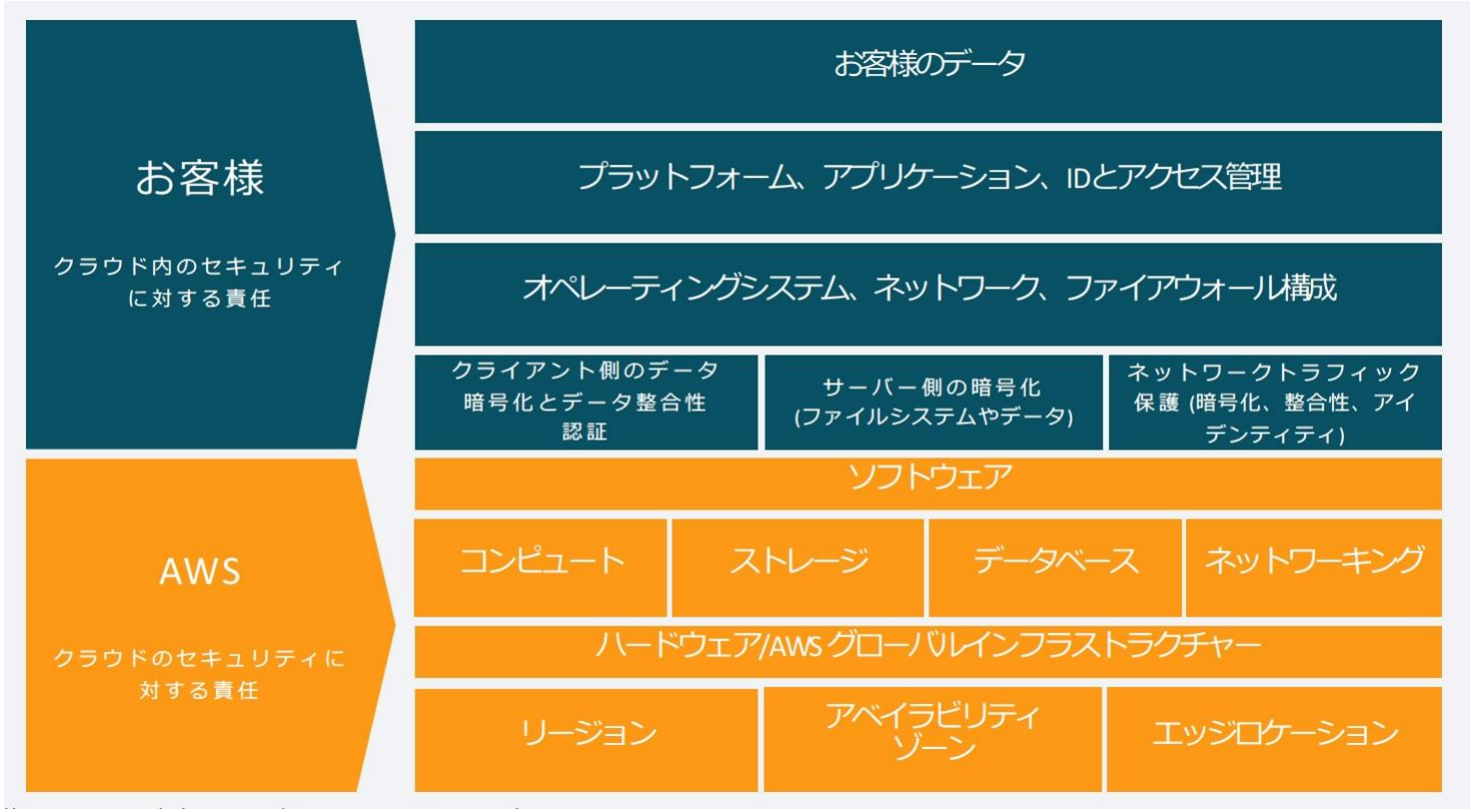
Safingサービス概要

- Safingは、AWS環境の脆弱性や脅威を一元管理できるサービス
- 知見がないと使いこなしにくいAWSセキュリティサービスの活用をサポート
- 脆弱性や脅威の検出だけでなく、対処方法まで見える化することにより、セキュリティ課題解決を支援

Safing

AWSセキュリティの考え方

- AWS環境のセキュリティ対策は「AWS責任共有モデル」を前提に策定・実行する
- 具体的な責任範囲は以下の通り
- AWS責任共有モデルに則ったセキュリティ対策ができているか、確認できる仕組みが必要



セキュリティがユーザー責任となる例

- オブジェクトストレージ（S3）の公開設定
- インスタンスのOSへのパッチ適用
- IAMユーザーの権限設定
- Lambdaのコードの脆弱性

課題

概念は広く知られているものの、
多くは、日々の管理までできていない状況

※出展：AWS公式WEBサイト「AWSクラウドセキュリティ-責任共有モデル」
https://aws.amazon.com/jp/compliance/shared-responsibility-model/

AWSセキュリティサービスとSafingの仕組み

- ユーザーの責任範囲となるセキュリティ対策をするために、AWSセキュリティサービスの活用が効果的
- Safingは、4種類のAWSセキュリティサービスを有効化し、 Safing Consoleに脆弱性や脅威の情報を集約する仕組み
- Safingのご利用にあたり、有効化されるAWSセキュリティサービスは下記の通り

AWS Security Hub

- AWS のセキュリティチェックの自動化とセキュリティアラートの一元化をする機能
- S3の公開設定のミスやルートアカウントへのMFA設定漏れなどを可視化できる

Amazon Inspector

- CVE情報を元にリスクスコアを作成
- EC2 インスタンス、コンテナ（ECR）、Lambda 関数の脆弱性や、意図しないネットワークの露出がないか、自動でスキャン

Amazon GuardDuty

- 不正なアクティビティやマルウェアの感染を自動で検出
- 人による作業やサードパーティーのツールを必要とすることなく、AWS アカウントの脅威検出が可能

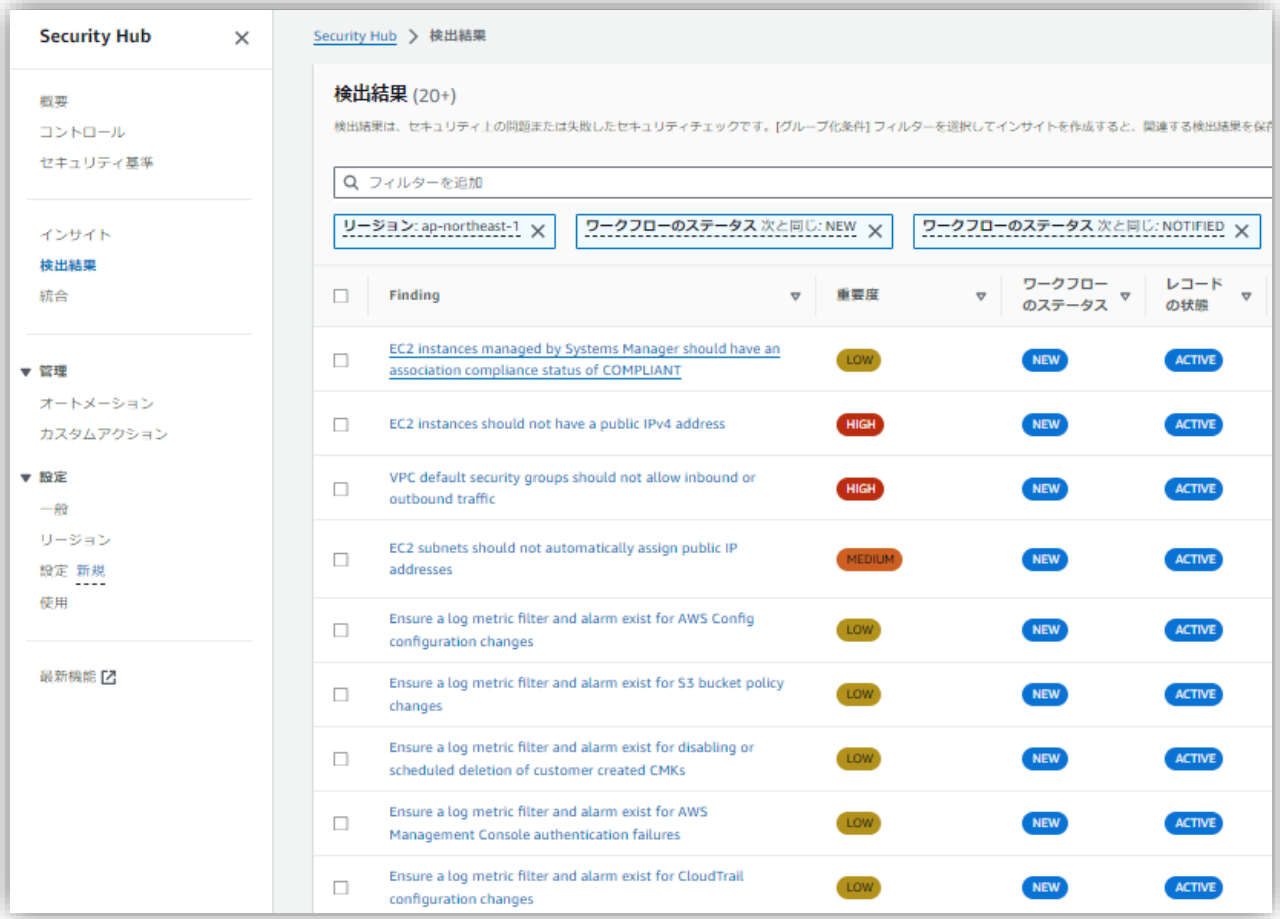
AWS IAM

IAM Access Analyzer

- IAM Access AnalyzerはAWS IAMの一機能
- AWSリソースに紐づいているポリシーを検査し、管理者として意図していない公開設定・IAM権限が設定がされていないか、自動で検出

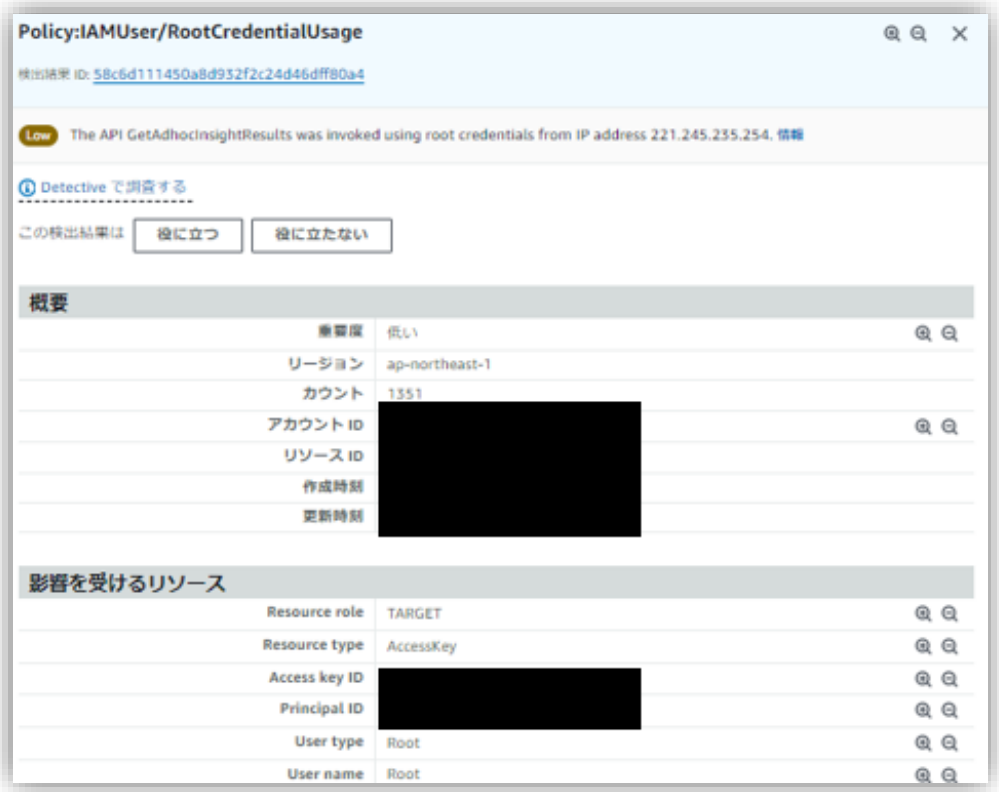
参考：AWS Security Hubのコンソール画面

- Security Hubでは、脆弱性が重要度ごとに表示されており、問題の内容が可視化される
- 改善方法が掲載されているページのリンクも掲載されており、修復対応を実行しやすい
- 英文で記載されており、和訳が必要（ブラウザによっては和訳ができない）
- Safingでは脆弱性情報・対策ともに日本語で表記されており、運用負荷の軽減・確認ミスの削減が可能



参考：Amazon GuardDutyのコンソール画面

- GuardDutyはセキュリティイベントを検出し、詳細が表示される
- 対応方法が記載されているリンクも掲載されるため、検出後、アクションに移しやすい
- 検出通知を受け取るためには、AmazonSNSやCloud Watchなどで設定をする必要がある
- Safingでは、電話番号およびメールアドレスを登録するだけで、GuardDutyで検出したイベントの即時通知が可能



ご活用イメージ

- Safingは、開発フェーズ・本番運用フェーズで発生しがちな課題に対応
- それぞれのフェーズにおける脆弱性管理課題は以下の通り

開発フェーズ

初期構築しながら
脆弱性をチェック

クラウドセキュリティ基準に
沿って開発が可能

不安から解消されて
開発スピードアップ

運用フェーズ

脆弱性管理コストを削減

状況の一元管理により
ガバナンス面を強化

事業全体への
セキュリティ対策の展開

Safingが活用できる
セキュリティインシデント例
①

Amazon S3バケットの公開設定ミスにより、情報漏洩

よくある問題

- Amazon S3の公開設定の誤りにより、外部から格納データの閲覧、編集が可能になっている（意図していない誤り）
- 格納されている情報に外部からアクセスされ、情報漏洩のインシデントが発生する

取るべき対策

- S3バケットの公開設定ミスを検出できる仕組みを持つ
- 誤った公開設定を修復する

Safingで出来ること

- 危険な公開設定がされているAmazon S3を検出し、Safingのコンソールにリソース情報や修復方法を反映

Safingが活用できる
セキュリティインシデント例
②

古いOS/ミドルウェアに重大な脆弱性があり、ウイルス感染

よくある問題

- 最新のOS/ミドルウェアにアップデートが行われていないため重大な脆弱性があるまま放置されてしまう
- 放置した結果、脆弱性を突かれた攻撃を受け、ウイルス感染などインシデントにつながる

取るべき対策

- 定期的にOS/ミドルウェアの診断をし、脆弱性を発見する
- 発見した脆弱性に対するアップデートを適用する

Safingで出来ること

- 古いOSやミドルウェアを検出し、重要度別に脆弱性を可視化し、対策・アップデート方法も案内される

Safingが活用できる
セキュリティインシデント例
③

不正なユーザー操作による暗号資産(仮想通貨)のマイニング

よくある問題

- 不正なユーザー操作により、仮想通貨のマイニングなど、リソースが大量に使われる
- 不正利用されたリソースの分、高額なクラウド利用料が請求される

取るべき対策

- 不正なアクティビティやマルウェア感染を検出する仕組みを設定する
- 不正な操作が発生した際に、すぐに気づき、対処できるようにする

Safingで出来ること

- 不正なユーザー操作が行われた場合に検出し、即時メールや電話で通知

Safingをご利用いただいているお客様

- 2024年7月時点で、Safingは100アカウント以上でご利用中
- Safingは大手企業から中小企業まで、幅広いお客様にお選びいただいている
- セキュリティの要望水準が高い金融機関にも採用されている

某大手保険会社 グループ企業様	**「Safingの導入により、毎月の脆弱性の確認はすべて自動化され、人手で確認する必要がなくなりました。 また毎月レポート化される為、発生した脆弱性に対して対処し次月には問題が解決されていることが明確に確認できるようになりました。」**
某携帯電話 事業者様	**「サービス立ち上げのスピードを優先し構築したがSafingで診断いただいた結果、様々な問題が明確になりました。 また、それらほとんどが自分達が認識していない問題であった為、 Safingを導入しない限り気づけなかったのではないかと思います。」**

料金プラン(税込み)

- Safingの利用料金は下記の通り
- Safing運用をご依頼いただくことも可能（別途料金がかかります）

※Safing運用をご要望いただく場合は、Safingの「お問い合わせ」よりご連絡をいただき次第、御見積いたします

	ベーシック 安心できるセキュリティ対策の可視化を必要とするチームに。	ビジネス あらゆる規模のセキュリティ対策を強化するチームや企業に。	エンタープライズ より高度なセキュリティのサポートを必要とするチームや企業に。
月額料金(AWSアカウント単位)	**¥9,900**	**¥13,200**	**¥26,400**
登録AWSアカウント上限数 (プロジェクト単位)	50	200	1000 最低利用10アカウント以上
対応策の提示	✓	✓	✓
脆弱性レポート	✓	✓	✓
脅威攻撃通知	-	✓	✓
自動コール	-	✓	✓
メールサポート	✓	✓	✓
電話サポート	-	-	✓
24時間365日サポート	-	-	✓
ユーザ登録数	10名	100名	1000名
支払方法	請求書払い	請求書払い	請求書払い

ご利用までの流れ

- Safingのホームページからプロジェクトの作成後、AWSアカウントを連携いただくだけで開始可能
- AWSアカウント連携はクラウドフォーメーションやスクリプトにより、自動で完結

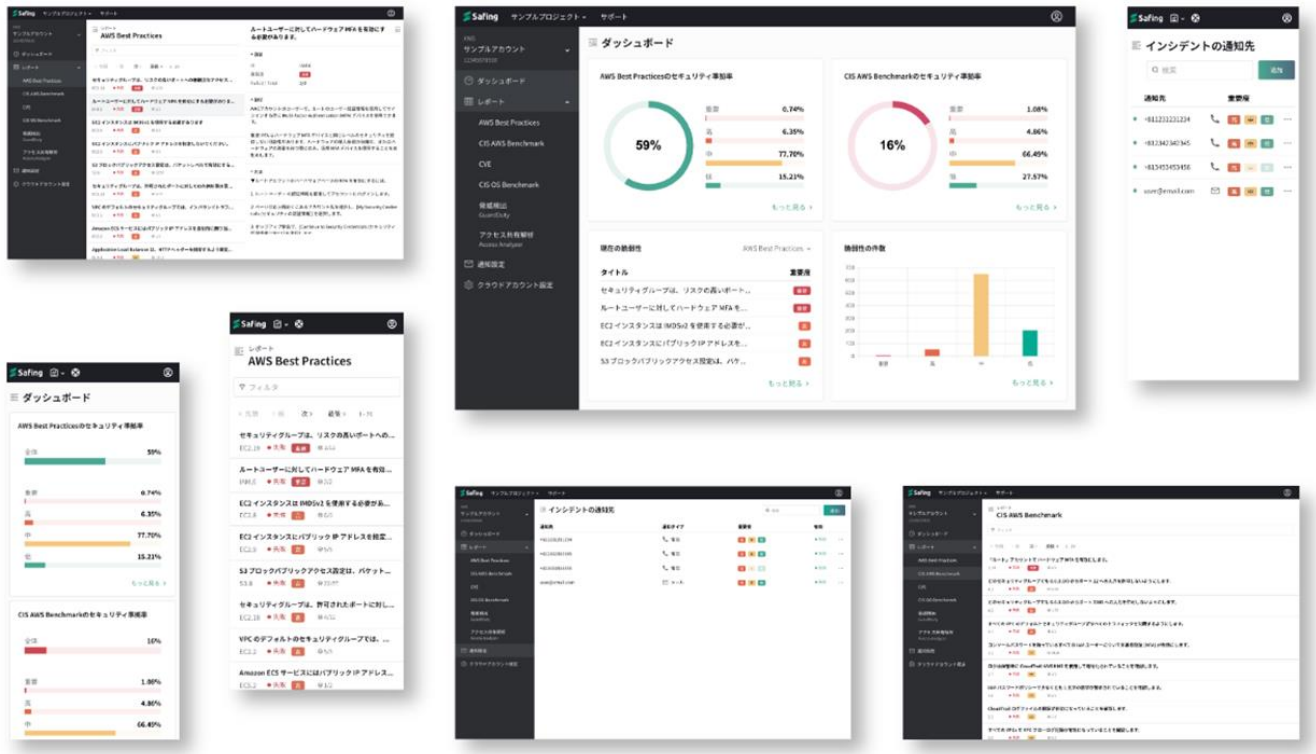
※AWS環境にてOrganizationsを利用している場合は、機能の有効化フローが異なるため、問い合わせフォームよりご連絡ください

※参考：Safingが利用する権限
SafingFAQ：IAMロールのsafing-access-roleが利用する権限は何に利用されますか？

Safing(セーフィング)で
クラウドセキュリティを一元管理

Safingは、AWSを安全に利用し続けるために、クラウドセキュリティをまとめて管理できるサービスです。

Safing



Safingをご利用いただくことで、
AWS Security HubやAmazon Inspectorによる
脆弱性情報や、Amazon GuardDutyや
IAM Access Analyzerが検出する脅威通知を
まとめて管理できます。
サービスの詳細情報はこちら

無償トライアル実施中

詳細は次のページ

AWS Summit Japan限定 Safingクーポン

Safing

AWS Summit Japan 2024

来場者特典

最大3カ月無料
トライアルクーポン

お問合せフォームにキーワードを入力いただき申請いただくと
ご利用開始当月+2カ月間、Safingビジネスプランを無償でご利用いただけます。

こちらから申請!

キーワード：ASJ2024

有効期限：2024/12/15
裏面の申請方法をご参照の上、
お問合せフォームより申請ください。

https://safing.com/ja/

JIG-SAW

JIG-SAW株式会社
〒100-0005 東京都千代田区丸の内1丁目4-1丸の内永楽ビルディング23F
03-6269-9810 （受付時間 平日9:30−18:30）

申請方法

STEP 01 https://safing.com/ja/ へアクセスし「導入前のお問合せ」をクリック

STEP 02 「お問い合わせ内容」に表面のキーワードを入入力し「送信」

STEP 03 お問合せ時に入力いただいたメールアドレスに
プロモーションコードと開始手順をご案内いたします。

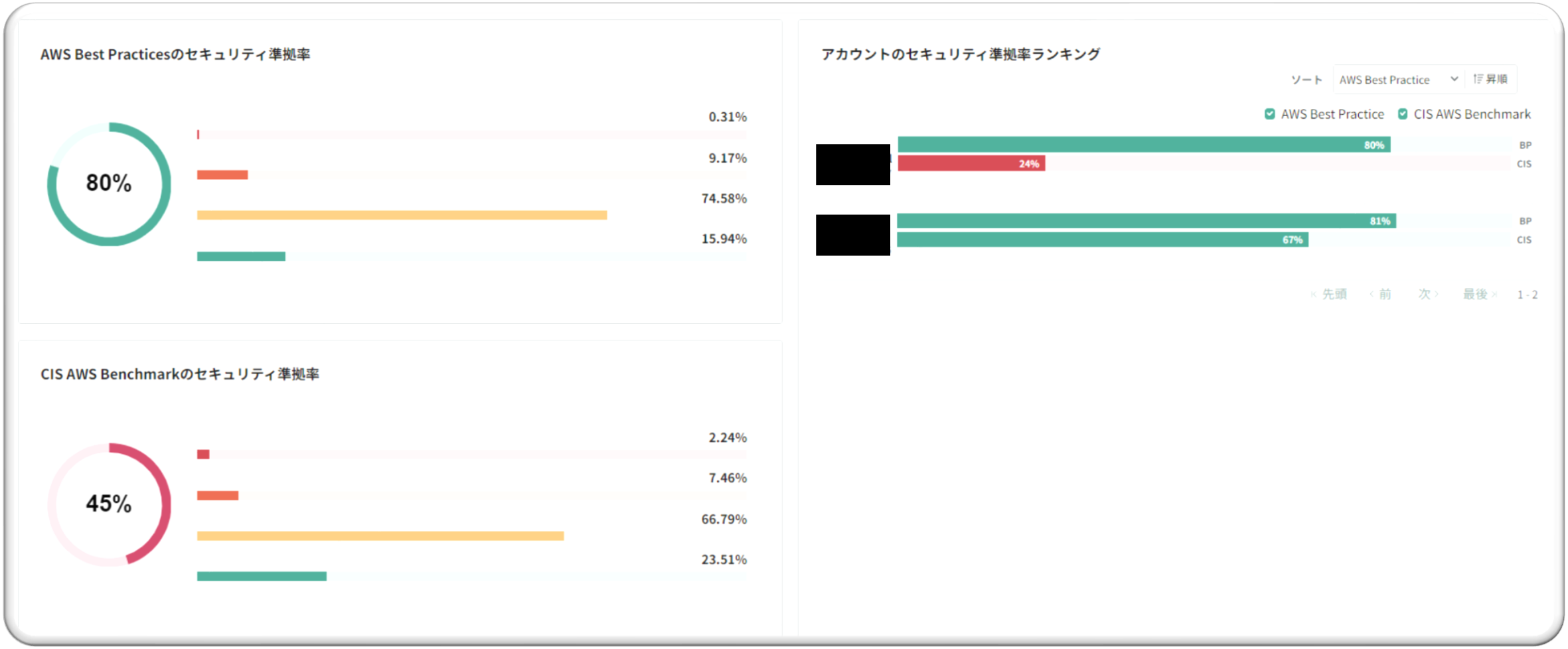
Safing

本日中に、メールにてアンケートをお送りします

APPENDIX

（開発中/リリース前）Safingグループ機能

- 複数のAWSアカウントの情報をまとめて表示できる「グループ機能」をリリース準備中
- 7月下旬のリリース予定



参考：Inspectorのコンソール画面

- 最新情報に基づくOSやミドルウェアの脆弱性が重要度別に可視化される
- 対策含め記載されており、アップデートの必要箇所が分かる